Listing of Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claim 1: (Currently Amended) A method of authentication for Media Gateway, characterized in that the method comprises:

~~setting up an initial key for~~providing each of a Media Gateway and a Media Gateway Controller with an initial key to ~~validating~~ validate ~~initial~~ digital signatures ~~between a Media Gateway and a Media Gateway Controller~~;

each of said Media Gateway and said Media Gateway Controller generating a shared key having a specific lifetime when said Media Gateway registers with said Media Gateway Controller using said initial key;

~~generating a new shared key having a specific lifetime by performing signaling communication between said Media Gateway and said Media Gateway Controller with said initial key;~~

said Media Gateway Controller and said Media Gateway authenticating each message between the Media Gateway Controller and the Media Gateway by using the shared key; and

~~authenticating calls and responses between said Media Gateway and said Media Gateway Controller with said new shared key; and~~

said Media Gateway and said Media Gateway Controller updating said shared key ~~between said Media Gateway and said Media Gateway Controller if~~when the lifetime of said shared key is expired.

Claim 2: (Currently Amended) The method according to claim 1, characterized in that the step of each of said Media Gateway and said Media Gateway Controller generating ~~a new~~the shared key ~~further~~ comprises:

the Media Gateway sending~~initiating~~ a register signaling message ~~from said Media Gateway~~ to said Media Gateway Controller ~~to register~~, wherein said register signaling message includes~~has~~ a parameter for said Media Gateway Controller to generate the~~generating a~~ shared key and ~~a~~an initial digital signature generated by the Media Gateway using said initial key;

said Media Gateway Controller validating the initial digital signature generated by the Media Gateway using the initial key;

said Media Gateway Controller generating ~~a~~ the shared key based on the parameter in said register signaling message and setting ~~up~~ a lifetime of said shared key when the initial digital signature generated by said Media Gateway is validated ~~after said Media Gateway Controller has validated said Media Gateway with said initial key~~;

said Media Gateway Controller sending~~initiating~~ a modification command ~~from said Media Gateway Controller~~ to said Media Gateway, wherein said modification command ~~has~~ includes a parameter for said Media Gateway to generate~~generating~~ the shared key, a digital signature generated by said Media Gateway Controller using said initial key, and ~~a~~ the lifetime of ~~a~~ said shared key;

said Media Gateway validating the digital signature generated by said Media Gateway Controller by using said initial key; and

said Media Gateway generating the shared key based on the parameter in said modification command and setting ~~and setting up~~ the lifetime, when the digital signature generated by said Media Gateway Controller is validated ~~of said shared key after said Media Gateway has validated said Media Gateway Controller with said initial key~~.

Claim 3: (Currently Amended) The method according to claim 1, characterized in that the step of said Media Gateway Controller and said Media Gateway authenticating each message~~authenticating further~~ comprises:

for each call, said Media Gateway Controller attaching a digital signature generated by the Media Gateway Controller using said shared key to ~~each~~ a call message ~~from said Media Gateway Controller~~ transmitted to said Media Gateway ~~by using said shared key~~;

said Media Gateway validating said digital signature ~~in~~ attached to said call message ~~in said Media Gateway~~ by using said shared key, and ~~if it is valid,~~ returning a response message attached with a digital signature ~~using said~~generated by the Media Gateway using said shared key to said Media Gateway Controller when said digital signature in said call message is validated; and

said Media Gateway Controller validating said digital signature attached to~~in~~ said response message ~~in said Media Gateway Controller~~ by using said shared key~~, if it is valid,~~ and ~~setting up~~establishing a call connection~~service~~ when said digital signature attached to said response message is valid, otherwise denying the call.

Claim 4: (Currently Amended) The method according to claim 1, characterized in that the step of said Media Gateway and said Media Gateway Controller updating said shared key ~~further~~ comprises:

sending a notification command ~~from~~ by said Media Gateway to said Media Gateway Controller~~,~~ to request~~ing~~ said Media Gateway Controller to generate a new shared key, wherein said notification command ~~has~~ includes a parameter for said Media Gateway Controller to ~~generating~~generate ~~a~~ the new shared key and a digital signature generated by said Media Gateway using ~~an~~the initial key;

said Media Gateway Controller validating the digital signature generated by said Media Gateway using said initial key;

said Media Gateway Controller generating ~~a~~ the new shared key based on the parameter in said notification command and setting ~~up~~ a lifetime of said new shared key, ~~after said Media Gateway Controller has validated~~when the digital signature generated by said Media Gateway ~~with said initial key~~is validated;

said Media Gateway Controller ~~initiating~~sending a modification command ~~from said Media Gateway Controller~~ to said Media Gateway, wherein said ~~modify~~ modification command ~~has~~ includes a parameter for said Media Gateway to ~~generating~~generate the new shared key, a digital signature generated by said Media Gateway Controller using said initial key and the lifetime of the new shared key;

said Media Gateway validating the digital signature generated by said Media Gateway Controller by using said initial key; and

said Media Gateway generating the new shared key based on the parameter in said modification command and setting ~~up~~ the lifetime, when the digital signature generated by said Media Gateway Controller is validated ~~of said shared key after said Media Gateway has validated said Media Gateway Controller with said initial key~~.

Claim 5: (Original) The method according to claim 2, 3 or 4, characterized in that the algorithm used to generate a shared key by said Media Gateway Controller and said Media Gateway is different from the algorithm used to generate a digital signature by said Media Gateway Controller and said Media Gateway.

Claim 6: (Original) The method according to claim 2, 3 or 4, characterized in that a field/packet of an expanded protocol is used to transmit said parameter for generating a shared key and said digital signature.

Claim 7: (Currently Amended) The method according to claim 1, characterized in that the lifetime of said shared key is time, or the number of times that said shared key can be used for authentication.